Internet Governance: From traditional to IPvX Ecosystem

Authors:

- Alexey Shkittin
- Nikolay Labaznikov

Project Contributors:

- Alexey Shkittin
- Nikolay Labaznikov
- Alexey Blagirev
- Sergey Mukhortov
- Alexander Timokhin

Introduction

Internet governance consists of a system of laws, rules, policies and practices that dictate how its board members manage and oversee the affairs of any internet related-regulatory body. [1]

The mean point of making Internet "decentralized" has led to Internet being a complicated network, connecting independently-managed smaller networks, which could not operate without the traditional form of centralized governance. Sounds weird, right? Of course one can tell there are samples of nearly independent networks, like in Russian Federation, North

Korea or China, but maybe that is not the independence we all dream about.

Current traditional governance

According to "Internet Governance Project" [2], the governance timeline starts at 1987. Let's review the timeline and try to count numerous involved parties:

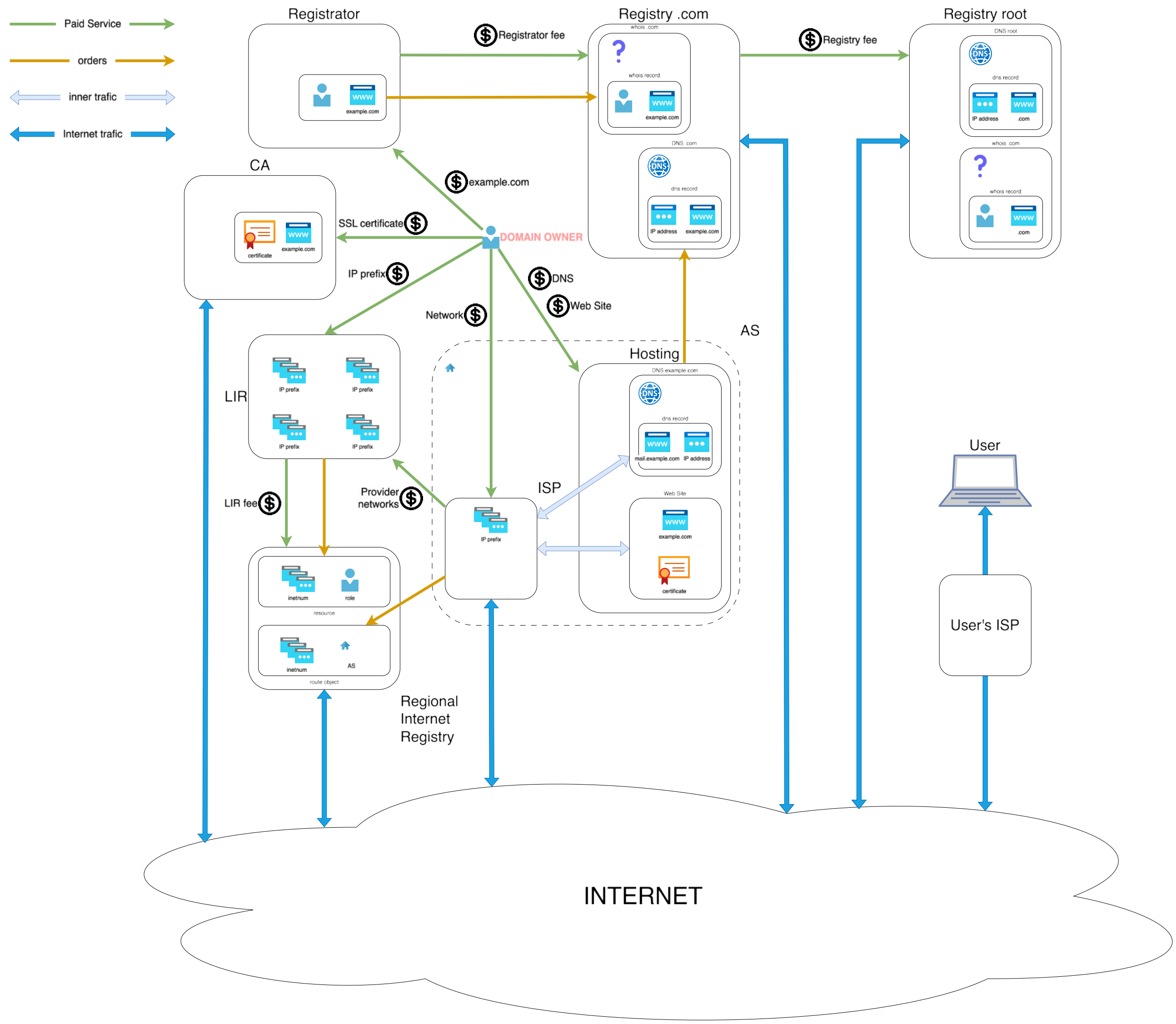
- 1987: IETF - Internet Engineering Task Force [4]
- 1989: RIPE - Réseaux IP Européens [5]
- 1990: IANA - Internet Assigned Numbers Authority [6]
- 1993: APNIC - Asia-Pacific Network Information Centre [7]
- 1994: RADb - Routing Arbiter Database [8]
- 1997: ARIN - American Registry for Internet Numbers [9]
- 1998: ICANN - Internet Corporation for Assigned Names and Numbers [10]
- 2002: LACNIC - Latin American and Carribean Internet Addresses Registry [11]
- 2003: WSIS - World Summit on Information Society [12]
- 2004: AFRINIC - African Network Information Centre [13]
- 2006: IGF - Internet Governance Forum [14]
- 2010: NANOG - North American Network Operators Group [15]
- 2014: NMI - NETmundial Initiative [16]
- 2016: PTI - Public Technical Identifiers [17]

This is just the tip of the iceberg, how many parties are involved. Just plus here:

- Domain Name Registries [18]
- Internet Service Providers (ISP) [19]
- Hosting Companies [20]
- Internet Exchange Points (IXP) [21]
- Copyright and Trademark Holders
- Streaming Platforms [22]
- etc.

all of those, who actually maintain and transmit the Internet content.

When you start your own business and apply a website, you have to dive into situation described by this simplified diagram, representing the core parts of administrative and technical Internet governance complicated process.



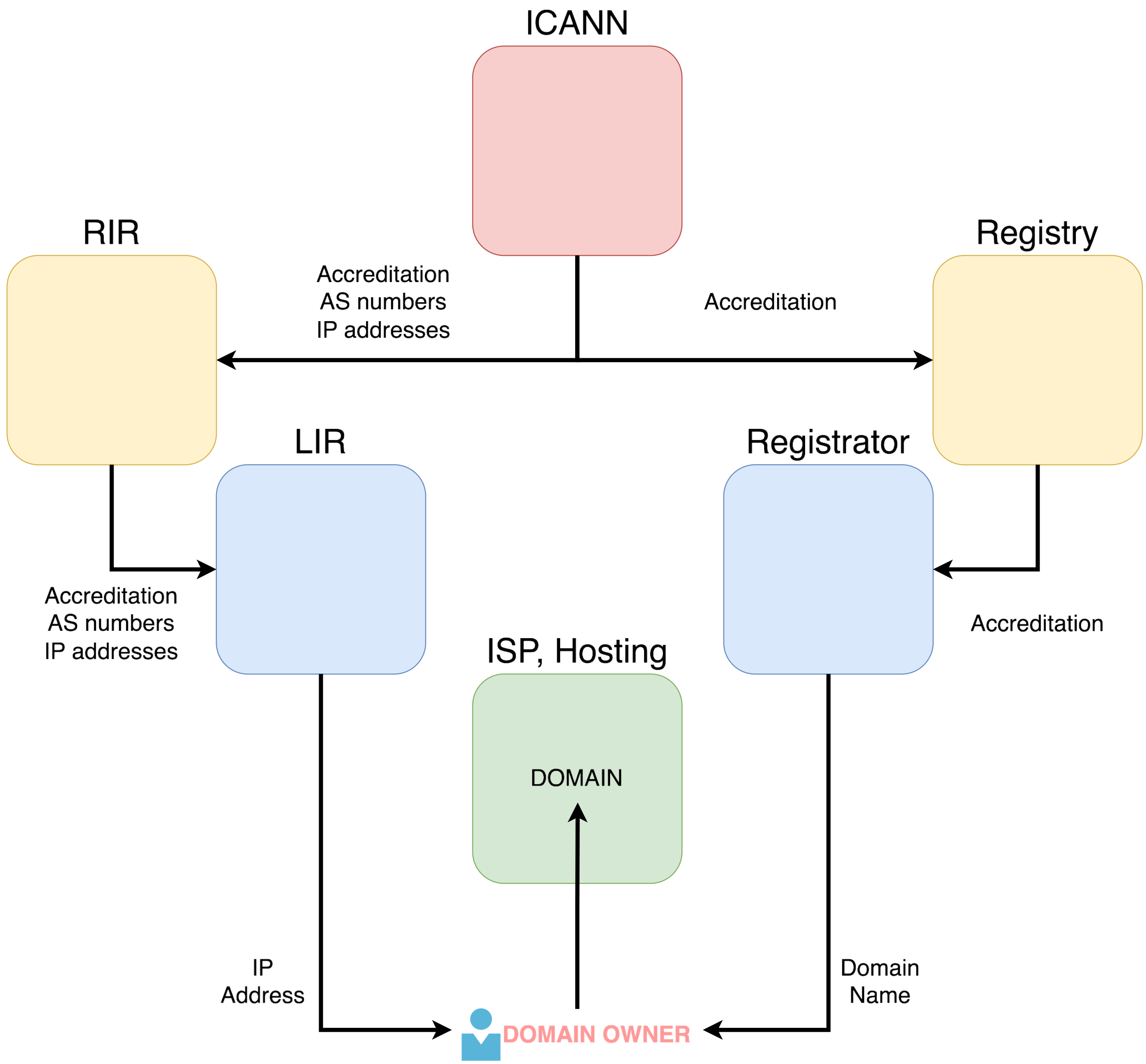
Root-level

Let's take a look at the administrative part of the Internet. Talking frankly - who rules?

TLDR; ICANN is at the top, and this affects any of the underlying activities. [23]

"ICANN also has responsibility for managing toplevel assignment of the numeric Internet Protocol (IP) address space and for administration of a number of registries for parameters and their values associated with the Internet protocol suite." [23] and things haven't changed recently.

The multi-step process on applying your website, simplified:



Top-level

.com, .org, ,net, ...

Though there are numerous parts involved in making your website up and running, the core of them depends on ICANN:

- ICANN distributes Autonomous Systems among RIRs (this relates to your Internet Service Provider)
- ICANN distributes IP address blocks among RIRs (this relates to your website

- address)
- ICANN accredits Generic Top Level Domain Registries and New Generic Domain Name Registries (this relates to you website domain name)

The RIRs (Regional Internet Registry) [24] are:

- ARIN
- RIPE NCC
- APNIC
- LACNIC
- AFRINIC

The examples of Registries [25]:

- .com : "VeriSign Global Registry Services"
- .org : "Public Interest Registry"
- .global : "Identity Digital Limited"
- .online : "Radix Technologies Inc."

2nd-level

example.com, ...
Your website usually belongs here. The cost you pay in total includes of all the commissions paid by the upper-level parties.

Traditional Model

The Traditional Model relies on addressing information governed by ICANN, RIRs, Local Internet Registries (LIR) [26], ISPs, Domain registries, Hosting providers, Certificate Authorities:

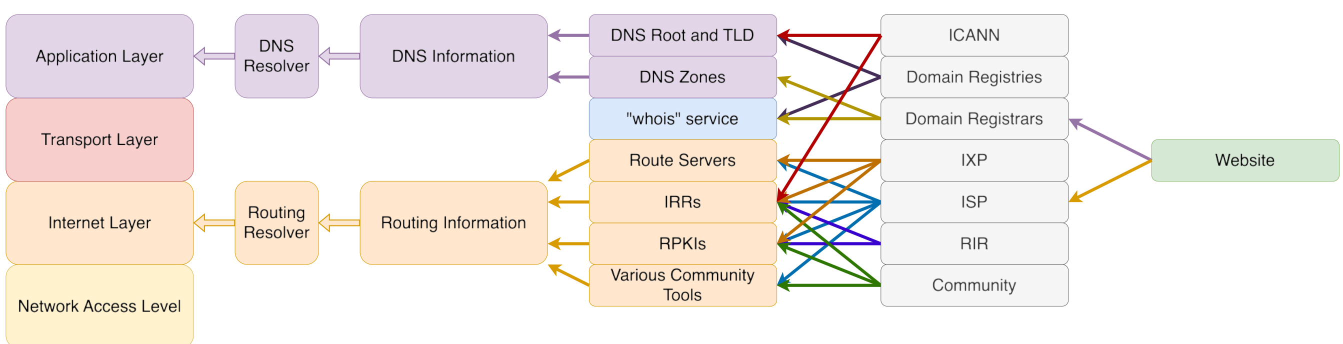
- ICANN: Global addressing and resource allocation and accreditation of RIRs and Domain Registries
- RIR: Resource allocation to LIRs and running databases
- LIR: Resource allocation to ISPs
- ISP: Resource allocation to clients
- Domain registries: Domains allocation to clients Maintaining DNS system [27] within own area of responsibility

- Hosting providers: Running users websites
- Certificate Authorities: Running certificates

When you apply your Website to a network, you have to interact with the main entity - ICANN. Actually, you address your needs to a hosting provider (or a Registrar), who usually provides necessary services all-in-one: ip address (or a small network), datacenter resources, domain name, DNS-server, etc. But it all comes down to mentioned ICANN who is the root source of the IP addresses and a DNS-system.

Let's take a look at current Internet protocol stack. We choose TCP/IP model [28] as a better fit:

- Application Layer
    - Everything related to data to be transmitted
- Transport Layer
    - Here apply protocols, responsible for data fragmenting, preparing for transmission, and putting back data together again
- Internet Layer
    - Protocols for reliable data delivery
- Network Access Layer
    - Layer representing the hardware and media



(Technically, the Internet is capable of running without the DNS information at all, so the top part of the diargam is initially redundant. But of course we cannot afford the absence of such a convenience.)

Let's summarize the steps being followed when applying a Website:

- You contact a hosting provider (plus it often acts as a Domain Registry) for a website with an **IP address** and **Domain Name**

- You order a resource at a datacenter or you bring your own devices to a datacenter and provide ISP with your **IP address**
- Usually, you host your DNS server at your ISP side, so you provide your **Domain Name** too
- According to your address information and domain information, ISP fills the **Routing Information** and the **DNS Information**, that will be propagated across the Internet, so other network devices could reach your site
    - The mandatory source for all routing devices is the Internet Routing Registry Database (IRR) [29]. Each of the Regional Internet Registries runs it's own IRR db, which contains information about that RIR-assigned networks (assigned to RIR by ICANN). You and ISP fill the **Routing Information** in IRR db:
        - you fill your part of the information in IRR db, that ISP now rules your network
        - ISP fills it's part of the information in IRR db with you network route objects, pointing to ISP ASn
    - As a DNS hoster, ISP fills your **Domain Name** information in DNS system
- Your **Domain Name** information is being propagated across the Internet by the protocol means
- Your **Routing information** is also propagated across the Internet by the means of being published to several databases - the abovementioned IRR and optionally:
    - Route Servers at Internet Exchange Points (IXP), where your ISP participates
    - Resource Public Key Infrastructure (RPKI) [30], used by your ISP to proof the validity of your **Routing Information**
    - Community-driven tools, registries, and databases - the Community uses various scanners and crawlers to snapshot Internet routing state, increase validity and trustworthiness of resources in Internet

What do DNS and Routing information serve then?

- **DNS Information** serves as a source for Application Layer in our model
    - When an Application wants to address a Website, it refers to the DNS-system to know the IP Address of a requested Website
    - This IP Address is passed then to the Internet Layer of our model

- Routing Device runs at the Internet Layer. It has the **Routing Information** loaded, so it knows where to send your data, when you communicate with an IP Address of a Website

Using Blockchain

The Internet grew from a small network, overcoming limitations of scalability and centralized government. That was a story of "applying patches" from the beginning.

The main technologies grew from limitations:

- NAT [31]
- BGP [32]
- IPv6 [33]
- QoS [34]
- VPN [35]

and insecurity:

- SSL / TLS [36]
- DNSSEC [37]
- IPsec [38]
- Digital signatures [39]

With the network growth, distribution of network resources from the network center had made the center being not capable to maintain this function on own behalf, so it started delegating duties.

You see how many parties are involved, and they run various databases. There are also numerous entities that change DNS and Routing information. It might be useful to store some of these databases information in a blockchain [40].

Modern technologies have to implement security by design. Using blockchain as a source of proof allows to minimize the number of involved parties, because at nearly every network model layer we face the necessity to authenticate and authorize actors. The single blockchain keypair could take it all.

Using the blockchain as a single but distributed source of routing and addressing information

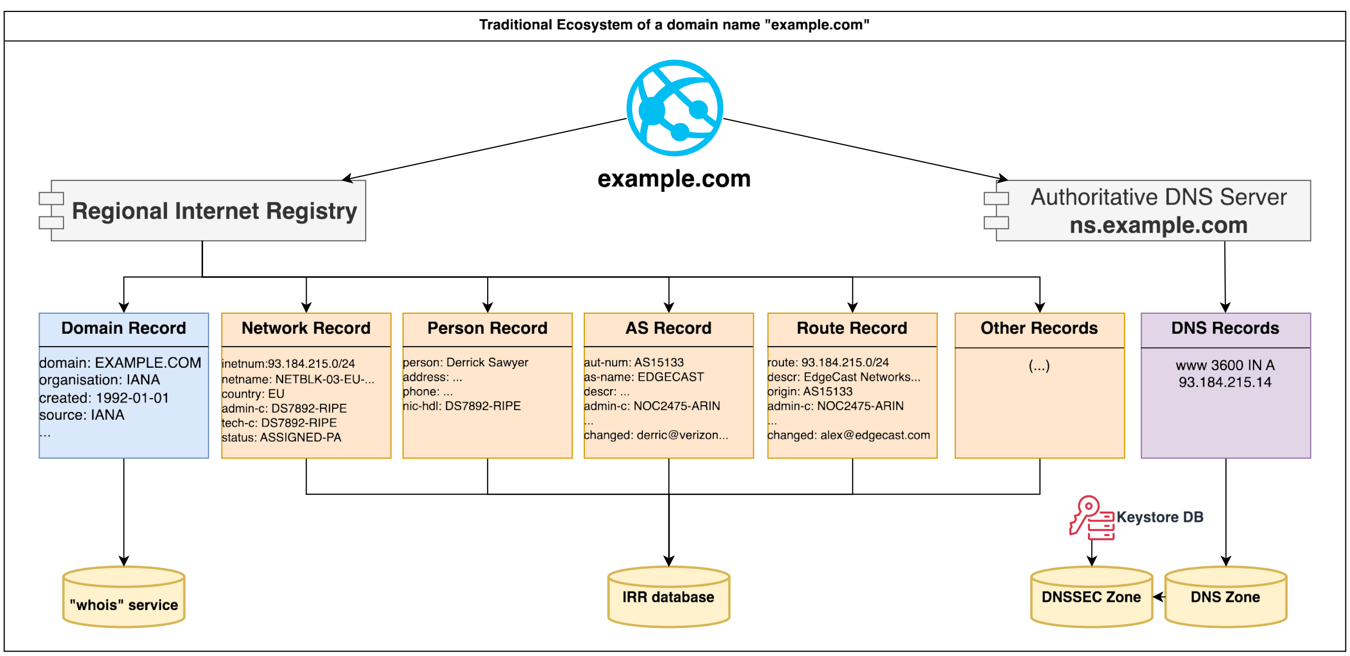
could also leverage limitations of the traditional scheme.

We can point out several major steps of incorporating blockchain to this scheme:

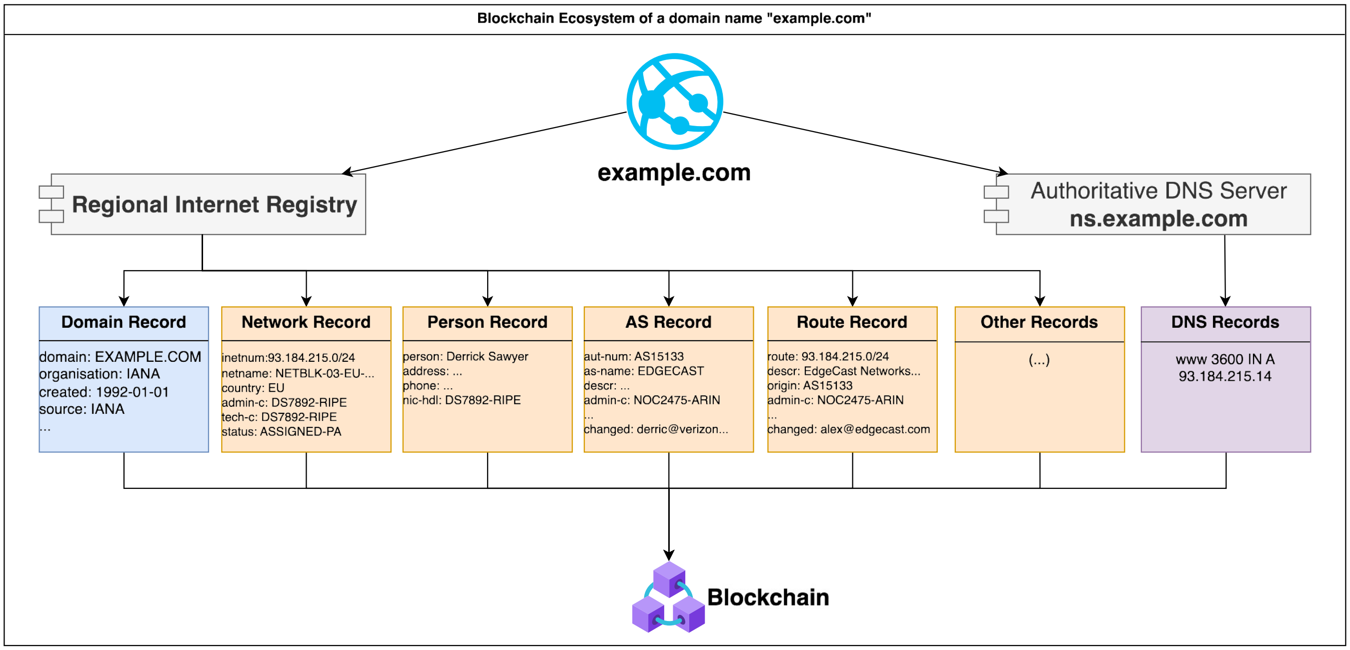
- Database shifting
  - Blockchain introduced
  - Actors move their databases into blockchain
  - Bridge and modified resolvers introduced
- Direct interaction
  - Resource owners reject the traditional way and interact directly with the Blockchain
- Obsolete DNS
  - DNS system becomes non-actual due to zoneless domain name usage

Database shifting

The traditional way is to maintain numerous databases run by responsible actors.



Next, the framework of using blockchain as a distributed database is introduced. The involved parties are still the same but they store their database information in a blockchain.



Because now we have databases info contained in the Blockchain, we need new bridges and resolvers capable to interact with it to insert into Blockchain or query.

DNS Resolver for Blockchain

When an application sends data to the Website, it uses operation system's built-in dns-resolver code. With the information contained in yet unusual Blockchain storage, the Application needs somehow query it. Unless the operation system is enabled by Blockchain interaction support, this can be done in several ways:

- browser extension
  - new custom scheme [41] introduced "ipvx://"
  - new scheme is supported by browsers
- modules for programming languages
  - bring possibility to add Blockchain interaction directly to application code
- 3rd party OS drivers
  - the driver is installed into OS
  - applications interact with OS as usual

Routing resolver for Blockchain

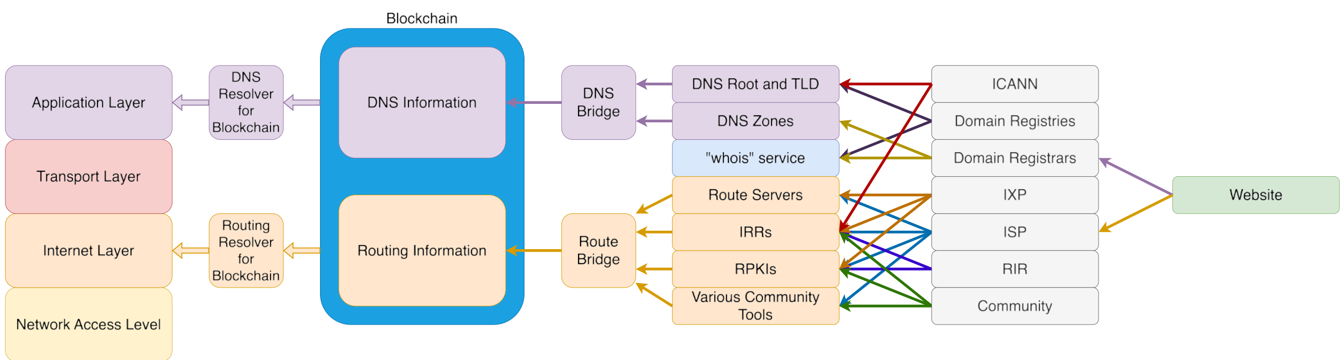
Internet Layer is represented with various routing-capable devices across the network - Routers [42]. Routing information has to be configured and uploaded to a router. In traditional

scheme building routing information means to run self-designed or enterprise-ready software, that queries databases with routing information, prepare configurations and inject routers with these configurations.

In blockchain-enabled scheme things are still the same as in traditional one, except for the software to build configurations has to be upgraded with ability to interact with the Blockchain.

Bridges

Similar to the situation at resolving side, the actors has to insert information into the Blockchain, so the software used for traditional database interaction has to be upgraded with blockchain interaction ability.



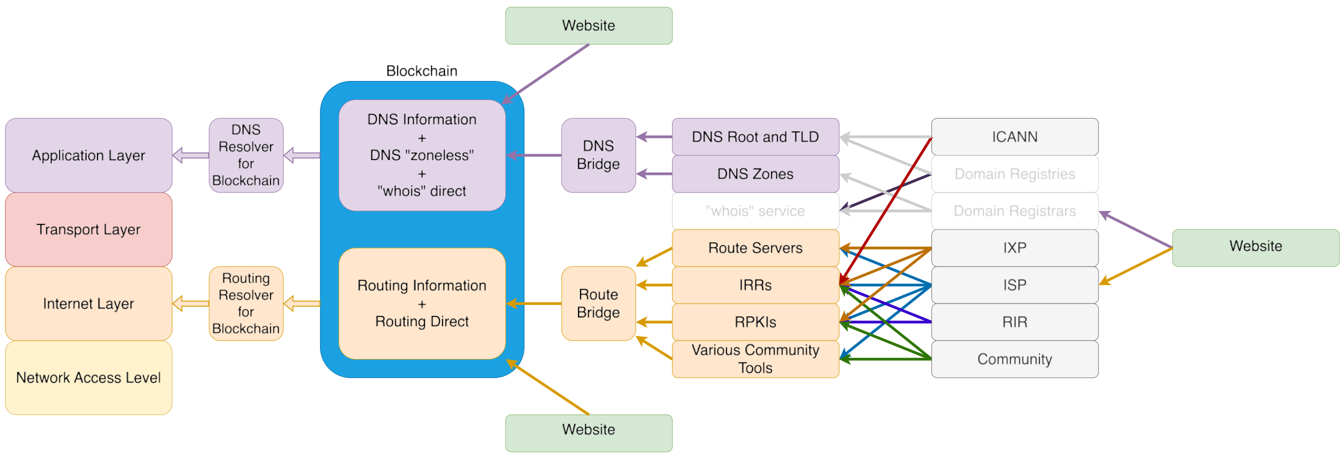
Direct interaction

Resource owners (the Website) begin to use the Blockchain directly, involving non-traditional mechanisms of ownership approval.

In the traditional scheme, when you need to proof your ownership (as a legal owner), you come in-person to the service provider, and it issues some kind of authenticator for you. For Certificate Authority it is the digital certificate [43], and you use digital signatures then, or it can be a certificate for your website, and you proof the validity of the website. For an Internet Service Provider this authenticator is a route object, pointing to your Person IRR database record. For Domain Registry it is a Whois Database record with your contact attached to domain information, etc.

When transmitting ownership data from traditional databases to Blockchain, the Website could perform additional authenticative actions, that the Blockchain expects him to pass to proof new blockchain records validity. For example, it could be a Person record in IRR

database, pointing to the public key, used to sign blockchain transactions. Or a DNS TXT record with a value of such key. No matter how, but as Internet in general relies on authenticity of the information from such databases, the transitional authenticity could be approved online.



Without traditional databases

Next, let's remember the beginning. The DNS system had no domains, subdomains, roots. Only the flat system with machine hostnames. It is clear, that with rapid grow, it became extremely hard to maintain and keep the DNS files updated across all of the network devices - again the delegation came, and a new protocol to sync info across DNS-servers.

With Blockchain **DNS "zoneless"** concept introduced - there is no need to strictly follow top-to-bottom domain hierarchy. When flat, the single "zone" could be filled up with information pointing to a desired short name of a blockchain identifier, probably also pointing to an ip address of a resource. There is still a dot sign "." possible in DNS record name, but it has no special meaning any more (again).

As it was mentioned, the initial filling of the Blockchain with information about Websites could be done according to current Local Internet Registries information from their databases.

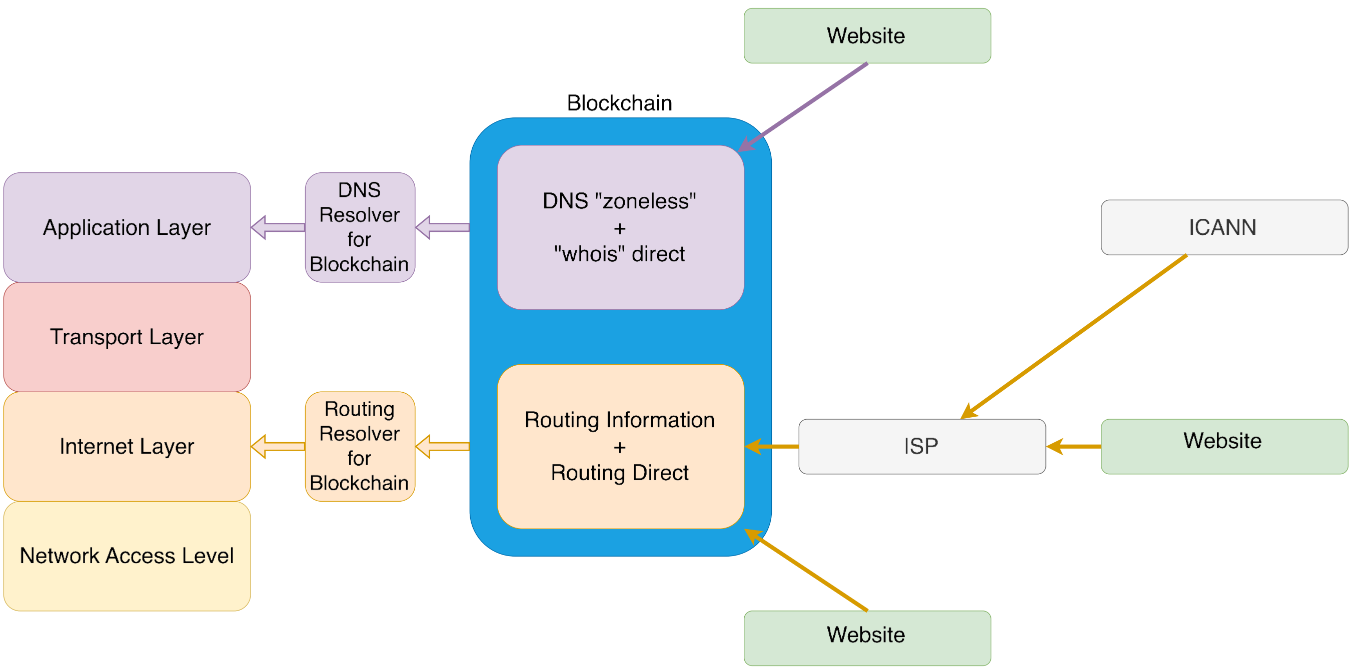
But how could we manage the situation, when multiple individual actors are willing to register similar names? There could be some models designed, imperially evaluating desired name and providing it to the actor in exchange for obligation to collaborate in blockchain. Occasional and sporadical registrations could be filtered out this way.

The route information could also be transferred into the Blockchain. The initial filling of the

Blockchain is possible with querying current route databases. Both the Website and an ISP could approve such records in the Blockchain.

Domain Registries and Domain Registrars traditional importance is declining. They could participate in this new scheme by registering valuable names on their own behalf, maintain these names by participating in the Blockchain and then transmit these names to clients for fiats for example.

In this new scheme there is no need to rely on traditional DNS hierarchy - it does not make sense, whether the Website uses TLD [44] or not.



Blockchain support layer

This is a development stage, when blockchain interaction functions run by dedicated applications, which we earlier called as **bridges** and **resolvers**, meet support by operation systems the applications are being run at.

Such support allows us to talk about the emergence of a new layer of the Network model - the **BCP Layer** ("Blockchain Control Protocol Layer").

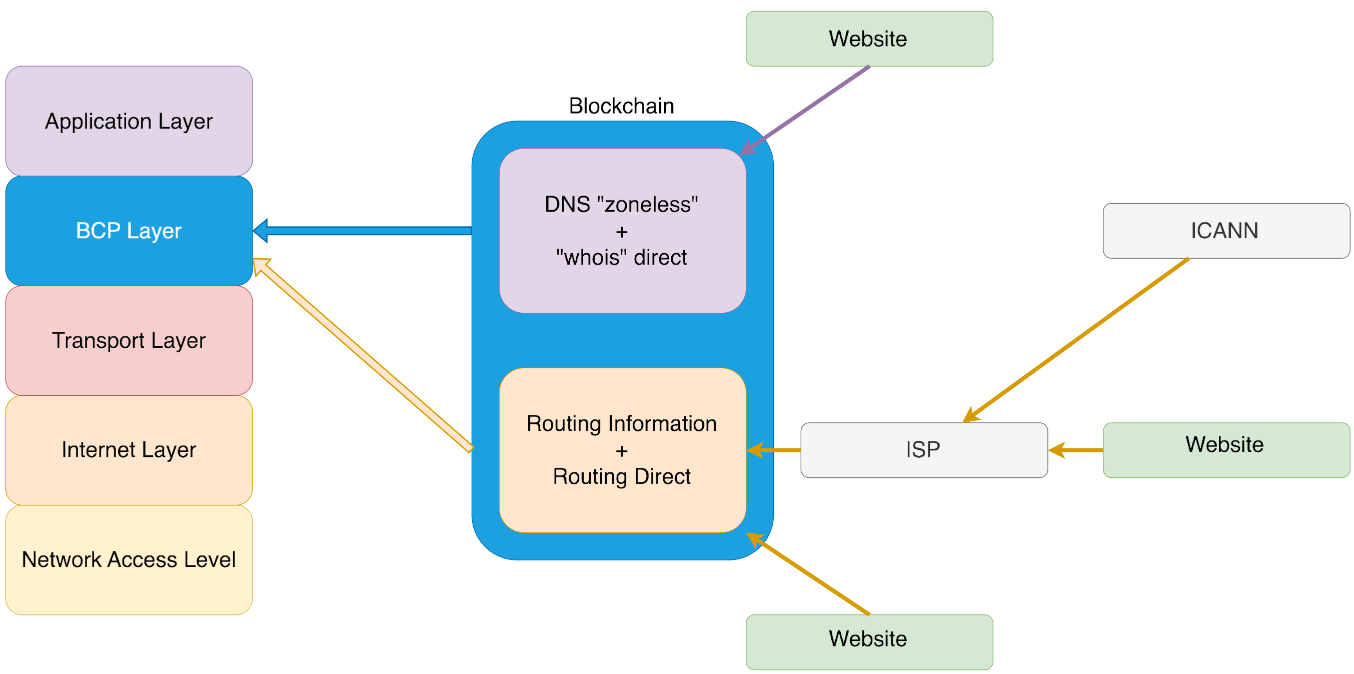
As the data from applications has to be passed further, the BCP Layer also takes functions of packaging application data into new type of packets [45] with blockchain-enabled addressing information added.

Functions of a new layer are:

- obtaining domain and routing information from the Blockchain
- forming BCP Layer protocol packets
- passing packets to underlying layer

Then an underlying layer uses it's own protocols to pass the data further, until the data meets physical layer, and the transmission reaches the destination network device.

At this development stage the underlying transport for BCP Layer is "Transport Layer" with well-known TCP Protocol ("Transport Control Protocol") ruling further transmission.



Blockchain control protocol (BCP)

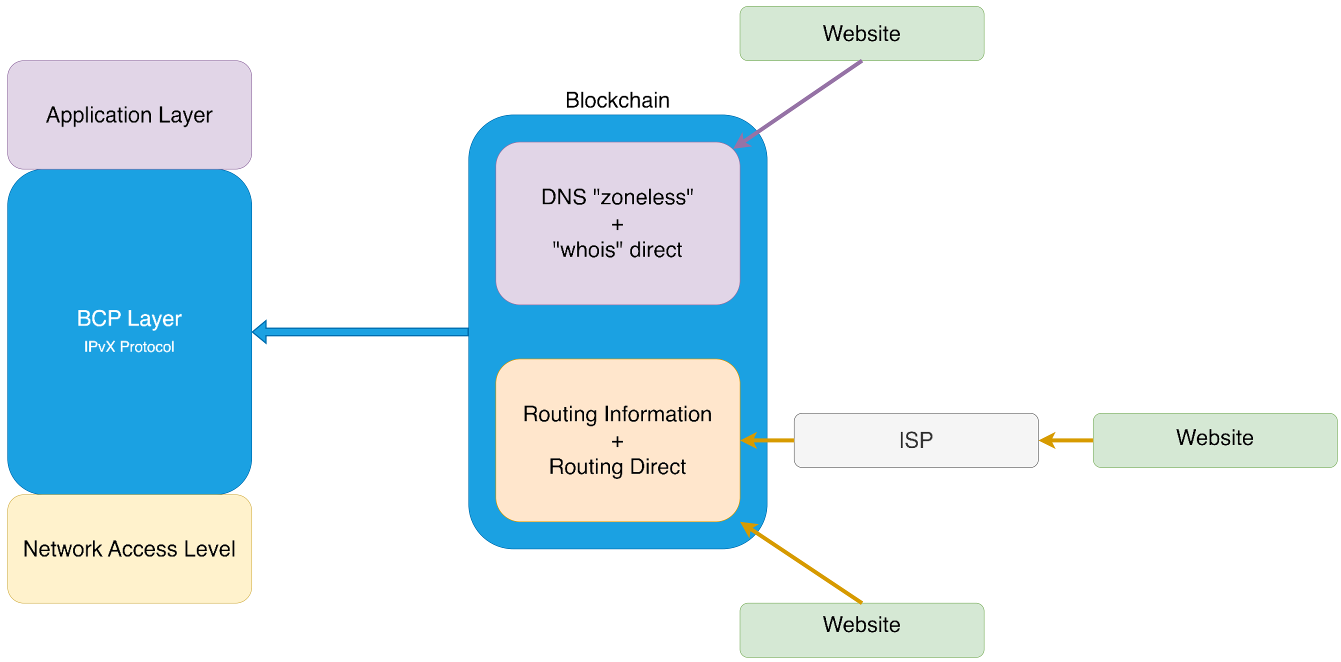
At this stage hardware devices capable to run BCP Layer and its supporting protocols are introduced.

As it was developed at the previous stage, applications send their data to BCP Layer and do not bother, what is beyond it.

And the BCP Layer is now capable of talking to hardware directly, taking BCP Layer protocols into play.

This design opens wide possibilities of bringing devices into network, because:

- there will be no nets to subnets hierarchy
- no root-tld-subdomain relations
- every BCP-capable device acts as a sole network node
- (even your laptop could run a temporary website immediately as you start it)



The Internet Service Providers continue to run their important function physically connecting devices to network, but there will be no need to maintain networks segregation any more, so they could focus on rapidly increasing Internet penetration, as numerous new devices will receive an opportunity to join the network.

What is IPvX?

We call the described concept "The IPvX Ecosystem".

IPvX is a new paradigm of Internet addressing, routing, and entity identification.

The goal is to power the described transition from traditional ecosystem with architecture, protocols, procedures, etc.

We need to provide these sufficient tools that will support and drive this paradigm shift. It is not just another version of IP protocol, upgraded to avoid some of already faced limitations, but a new network layer, abstract of underlying layers and lying closer to applications. That means no matter what type of a network you use, IPvX will run above it.

And with IPvX acceptance by the community and vendors there comes a possibility to implement new protocol to run hardware, meaning simplification of the Network OSI Model where applications interact with the new layer, and it in turn interacts directly with media transmission hardware devices.

All of the IP address already have their owner. There is no process of fresh allocations, but the constant process of transition of addresses from an old owner to a new one. Current state of ownership is fixed in RIR Databases and in DNS system information. This state could be transferred into the Blockchain and be controlled directly by the owners themselves later. There is no place for numerous registries of any kind in this paradigm - just the resource owners, the transfer media owners (ISPs) and datacenter owners (hosting and blockchains).

Of course, all of the presented diagrams describe models, that will run simultaneously for a long time. This transition will take time and maybe does not pretend to completely substitute current running network model, as it is suitable to most of the involved parties.

But new model brings new possibilities, and users of all kind will choose the one that suits them most. The more they value it - the more of them will join.

Our task is to design and provide clear roadmap on features, suitable usecases, new ideas of usage, and step-by-step instructions, so everybody could join and try.

Closer look at BCP and IPxV

Earlier we defined the transition from the traditional model to IPvX Ecosystem.

We defined new core components - the Blockchain and the BCP Layer.

BCP Layer

This is a new Network OSI Model Layer capable to interact with the Blockchain and use nested protocols for transmitting application data to underlying layers and further to the recipient.

The main idea is to "shift up" - provide an abstract from underlying transport layers, and use new types of addresses and routing information, aligned with the Blockchain usage. We could use the power of blockchain-related technologies to serve data delivery.

And at the next stage of development the BCP Layer will serve as a sole layer, which interacts

with the Blockchain, the Application, and the Network Access Layer (transportation media).

We define the IPvX Protocol, which will serve these needs.

Prior to overview the IPvX Protocol let's take a look, what entities exist alongside the Blockchain, which we could use in our concept.

Blockchain

The blockchain serves as a reliable, secure, and distributed database. When a database record is made the Blockchain stores this transaction with the following properties:

- authenticated [46]
- integral [47]
- non-repudational [48]

This means the transaction is made by the expected party, the transaction has not been changed on a way to the Blockchain, and the party performed the transaction can not cancel the transaction in meaning of the deletion.

All these properties belong to the Blockchain user number - the wallet number which is the public key of the user. And with the private key [49] the user signs their transactions.

And here comes the same story as with IP addresses and domain names. To link IP addresses with suitable domain names the DNS technology had been implemented.

The blockchain technology provides another possibility to link complicated user number with useful identity - **Non-Fungible Tokens (NFT)** [50]. Not only the identity, but any other entity.

Non-Fungible Tokens

Broadly speaking, NFT is a unique digital asset verified using blockchain technology, representing ownership and authenticity of a specific item, such as art, collectibles, or digital identity.

In relation to our model, NFTs could be used to proof identities of these entities:

- user
    - private person
    - legal entity

- network address
    - traditional IP address
    - new IPvX address
- alias to the address
    - traditional domain name
    - "zoneless" domain names, which we defined earlier in "Without traditional databases" section
- routing information
    - traditional AS numbers, route objects, and other information from IRR databases
    - new model routing information
- any other entity we want to reliably identify

Smart Contracts

Next, the blockchain provides a mechanism to establish the rules, how do entities interact - **Smart Contracts (SC)**. [51]

A smart contract is a self-executing contract with the terms of the agreement directly written into code, which automatically enforces and executes the terms on a blockchain when predefined conditions are met. So it is a program with some input and output data.

The input is:

- the agreeing parties
- the conditions of the agreement

The output is:

- the signing of the contract
- storing the signed contract on the blockchain

In relation to our model, SCs could be used for:

- allocation of network addresses
- allocation of aliases to the addresses
- changing routing information of any kind
- any other actions, where two parties agree in resource allocation

One new non-obvious SC use case - bringing **network security** [52] right to the core. We could describe **firewall rules** [53] at a network definition level. For example, we could allow or deny network access from one NFT to another - this is a revolutionary approach, because until now these actions were held on a client access level.

In relation to SC-defined routing rules, there is a second major new use case - parties cold agree on a **traffic transit**, and this brings new opportunities to the business.

Artificial Intelligence

With the rules described and relations between parties established, it is possible to query these rules with the help of the Artificial Intelligence [54].

In traditional model with TCP/IP stack various routing protocols are involved to choose mainly next hop for the single packet. The complete route of the packet is combined according to metrics used by these protocols, the rules for decision, where to send next from a given router, and interconnections between internet service providers.

Building route in IPvX Ecosystem brings new possibilities in terms not only next-hop rules, but also an ability to build or choose the best route to the destination, according to various agreements. For example, passing traffic from NFT1 to NFT2 through NFT3 could include some price. Also for some kind of traffic there could be establlished firewall rules, so the complete route has to be changed. Whatever affects, it could be evaluated and calculated to bring the best route to the sender, whether it has to be the cheapest route, the fastest route, or even the route, which would generate income for the sender.

So we can conclude, that routing becomes more complicated, and it is desirable to delegate this duty to the **Artificial Intelligence (AI)**.

Bringing the routing model to AI is up to the customer, or it could choose one of the models, offered by the **AI Services Provider**.

IPvX Protocol

This is a new protocol to serve addressing and routing, with classic packets layout.

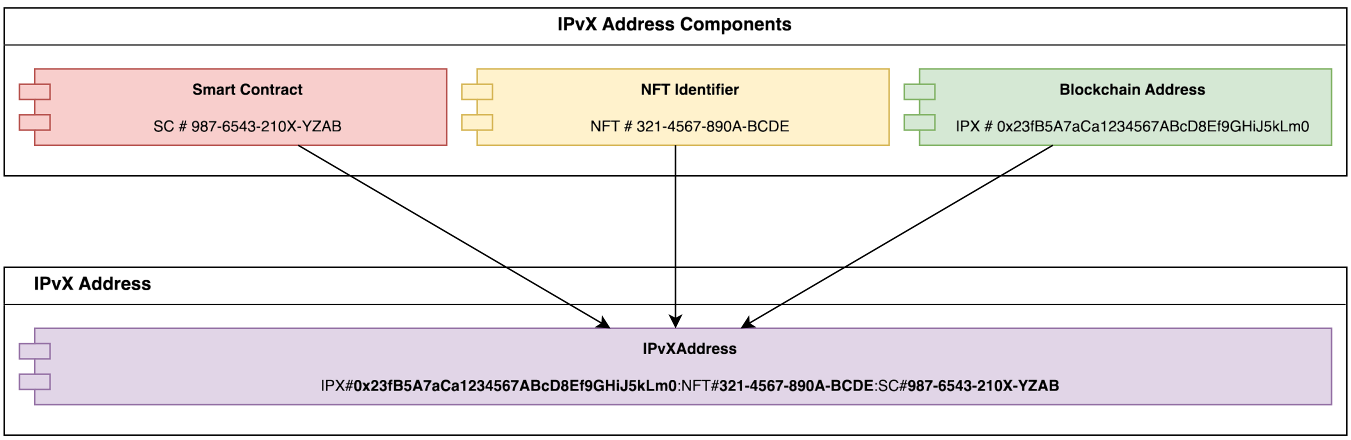
The structure and complete description of IPvX protocol is at the development stage, but we could highlight core components.

IPvX Address

As we described earlier in "Blockchain" module, the blockchain related technologies bring new features like routing and firewall to the network definition level. That's why the address now is not only an entity that serves to identify a destination point, but also a service or person (or whatever identified), hosting at the destination point, and a rule, defining the connection.

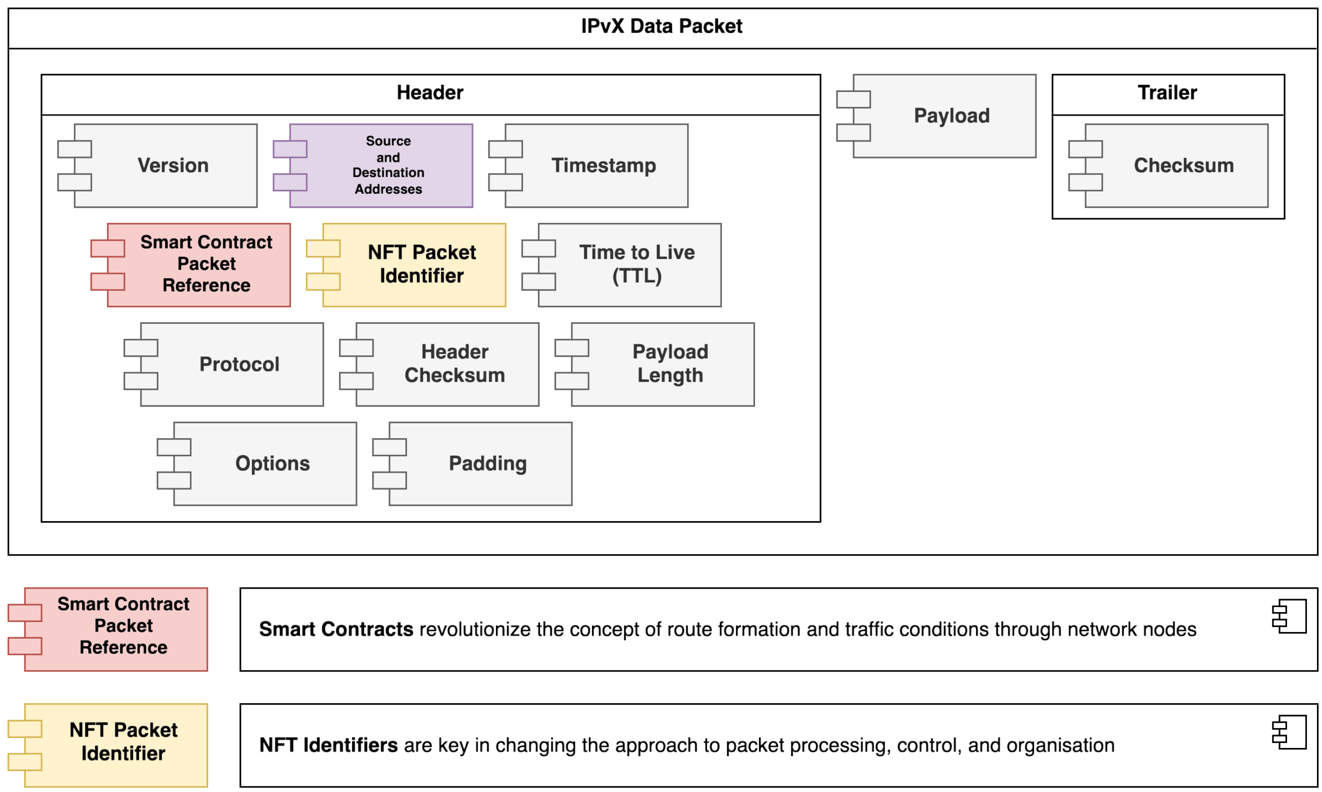
That's why we define an IPvX Address like a joint of these three identifiers:

- IPX (blockchain address of an interconnecting party)
- NFT (an entity, to which we address our packet)
- SC (a connection rule)



IPvX Packets

The variant of the packet structure could be represented with the diagram:



The json representation:

```
{
  "Header": {
    "Version": "IPvX v1.0",
    "SourceAddress": "IPX#1A2B3C4D:NFT-1234A789:SC-A1B2C3D4",
    "DestinationAddress": "IPX#9Z8Y7X6W:NFT-9876Z543:SC-Z9Y8X7W6",
    "Timestamp": "2023-08-07 12:34:56 UTC",
    "TTL": 128,
    "Protocol": "TCP",
    "Checksum": "AF38",
    "NFTPacketIdentifier": "NFT-1234A789",
    "SmartContractReference": "SC-A1B2C3D4",
    "PayloadLength": 512,
    "Options": "None",
    "Padding": 16
  },
  "Payload": "Hello, this is a sample message sent via IPvX from one device to another. Th
  "Trailer": {
    "Checksum": "D7E2"
  }
}
```


Headers

- Version Field: Pinpoints the IPvX version

Source and Destination Addresses

- These are dynamic in size and are structured to include the blockchain IPX address followed by NFT-based identifiers and smart contract references.

Timestamp

- Denotes the exact moment the packet was dispatched.

Time To Live (TTL)

- Illustrates the packet's remaining lifespan within the network.

Protocol Field

- Signifies the protocol overseeing the payload.

Header Checksum

- A safeguard ensuring error detection during transmission.

NFT Packet Identifier

- A singular identifier cementing traceability and packet distinction.

Smart Contract Packet Reference

- Paves the way for dynamic network operations by linking directly to a specific smart contract for packet transmission.

Payload Length

- Describes the extent of the packet's content.

Options

- Provides supplementary data or fields if necessary.

Padding

- Ensures the header adheres to a standardized length.

Payload

- A key component of a packet that carries basic data, such as messages, documents or even instructions.

Trailers

- This segment may encapsulate elements like checksums, underscoring the packet's authenticity while also signaling its conclusion.

We will cover the BCP Layer, the Blockchain, and IPvX Protocol in detail in future publications.

Conclusion

The IPvX Ecosystem proposal brings new possibilities to network management. New approaches of using the Internet arise, also bringing new potential business models.

New protocols with the power of AI could make a synergy and form a completely new paradigm of information transfer and sharing.

References

[1] Wikipedia "Internet governance" https://en.wikipedia.org/wiki/Internet_governance

[2] Internet Governance Project "What is Internet Governance?" https://www.internetgovernance.org/what-is-internet-governance/

[4] IETF Home Page https://www.ietf.org

[5] RIPE NCC Home Page https://www.ripe.net

[6] IANA Home Page https://iana.org

[7] APNIC Home Page https://www.apnic.net

[8] RADb Home Page https://www.radb.net

[9] ARIN Home Page https://www.arin.net

[10] ICANN Home Page https://www.icann.org

[11] LACNIC Home Page https://www.lacnic.net

[12] WSIS on UNESCO https://www.unesco.org/en/wsis

[13] AFRINIC Home Page https://afrinic.net

[14] IGF Home Page https://www.intgovforum.org

[15] NANOG Home Page https://www.nanog.org

[16] NETmundia Home Page https://netmundial.br

[17] PTI Home Page https://pti.icann.org

[18] Wikipedia "Domain name registry" https://en.wikipedia.org/wiki/Domain_name_registry

[19] Wikipedia "Internet service provider" https://en.wikipedia.org/wiki/Internet_service_provider

[20] Wikipedia "Web hosting service" https://en.wikipedia.org/wiki/Web_hosting_service

[21] Wikipedia "Internet exchange point" https://en.wikipedia.org/wiki/Internet_exchange_point

[22] Wikipedia "List of streaming media services" https://en.wikipedia.org/wiki/List_of_streaming_media_services

[23] ICANN "Strategy Panel: ICANN's Role in the Internet Governance Ecosystem" https://www.icann.org/en/system/files/files/report-23feb14-en.pdf

[24] Wikipedia "Regional Internet registry" https://en.wikipedia.org/wiki/Regional_Internet_registry

[25] ICANN Wiki "Registry" https://icannwiki.org/Registry

[26] RIPE NCC "Local Internet Registry. Training Course" https://www.ripe.net/media/documents/LIR-slides.pdf

[27] Wikipedia "Domain Name System" https://en.wikipedia.org/wiki/Domain_Name_System

[28] Wikipedia "Internet protocol suite" https://en.wikipedia.org/wiki/Internet_protocol_suite

[29] Internet Routing Registry Home Page https://irr.net

[30] RIPE NCC "Resource Public Key Infrastructure" https://www.ripe.net/manage-ips-and-asns/resource-management/rpki

[31] RFC1631 "The IP Network Address Translator (NAT)" https://www.rfc-editor.org/rfc/rfc1631

[32] RFC1267 "A Border Gateway Protocol 3 (BGP-3)" https://www.rfc-editor.org/rfc/rfc1267

[33] RFC2460 "Internet Protocol, Version 6 (IPv6) Specification" https://www.rfc-editor.org/

rfc/rfc2460

[34] Wikipedia "Quality of service" https://en.wikipedia.org/wiki/Quality_of_service

[35] RFC2764 "A Framework for IP Based Virtual Private Networks" https://www.rfc-editor.org/rfc/rfc2764

[36] RFC8446 "The Transport Layer Security (TLS) Protocol Version 1.3" https://www.ietf.org/archive/id/draft-ietf-tls-rfc8446bis-10.txt

[37] RFC9364 "DNS Security Extensions (DNSSEC)" https://www.rfc-editor.org/rfc/rfc9364

[38] Wikipedia "IPsec" https://en.wikipedia.org/wiki/IPsec

[39] Wikipedia "Digital signature" https://en.wikipedia.org/wiki/Digital_signature

[40] Wikipedia "Blockchain" https://en.wikipedia.org/wiki/Blockchain

[41] IANA "Uniform Resource Identifier (URI) Schemes" https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml

[42] Wikipedia "Router" https://en.wikipedia.org/wiki/Router_(computing)

[43] Wikipedia "Public key certificate" https://en.wikipedia.org/wiki/Public_key_certificate

[44] Wikipedia "Top-level domain" https://en.wikipedia.org/wiki/Top-level_domain

[45] Wikipedia "Network packet" https://en.wikipedia.org/wiki/Network_packet

[46] Wikipedia "Authentication" https://en.wikipedia.org/wiki/Authentication

[47] Wikipedia "Data integrity" https://en.wikipedia.org/wiki/Data_integrity

[48] Wikipedia "Non-repudiation" https://en.wikipedia.org/wiki/Non-repudiation

[49] Bitcoin Wiki "Private key" https://en.bitcoin.it/wiki/Private_key

[50] Wikipedia "Non-fungible token" https://en.wikipedia.org/wiki/Non-fungible_token

[51] Wikipedia "Smart contract" https://en.wikipedia.org/wiki/Smart_contract

[52] Wikipedia "Network security" https://en.wikipedia.org/wiki/Network_security

[53] Wikipedia "Firewall (computing)" https://en.wikipedia.org/wiki/Firewall_(computing)

[54] Wikipedia "Artificial intelligence" https://en.wikipedia.org/wiki/Artificial_intelligence

[#] https://www.dotmagazine.online/issues/digital-business-models-ecosystems/no-better-way-to-give/tokenization-of-internet-address-space